APPLICATIONS OF FREE PROBABILITY TO QUANTUM INFORMATION THEORY (Mathematical Studies on Independence and Dependence Structure : Algebra meets Probability)

AUTHOR(S):

COLLINS, BENOIT

数理解析研究所講究録
第1820巻 2012年 25-30

APPLICATIONS OF FREE PROBABILITY TO QUANTUM INFORMATION THEORY

BENOÎT COLLINS

ABSTRACT. We show how Free Probability Theory -and in particular, recent results regarding the norm convergence of random matrices- help to better understand important problems in Quantum Information Theory, such as the problem of Minimum Output Entropy additivity.

This is a report on joint papers and projects with Ion Nechita, Serban Belinschi, Camille Male and Motohisa Fukuda

1. ENTANGLEMENT AND ADDITIVITY

1.1. **Entanglement and entropy.** In Quantum Information Theory, a vector subspace C of a tensor product $A \otimes B$ of two Hilbert spaces is said to be *entangled* iff 0 is the only vector of C that can be written as $a \otimes b$ with $a \in A, b \in B$. The problems of quantifying entanglement, and of finding 'highly' entangled spaces are very important in quantum information theory.

For $x \in A \otimes B$, its *singular values* -also known as *Schmidt coefficients* in Quantum Information Theory- are non-negative numbers $\lambda_1(x) \geq \ldots \geq \lambda_k(x) \geq 0$ such that

$$x = \sum_{i=1}^{k} \sqrt{\lambda_i} e_i(x) \otimes f_i(x)$$

Here, $k = \min(dim(A), dim(B))$; $e_i(x)$, $f_i(x)$ are orthonormal vectors. The sequence $\lambda(x) = (\lambda_1(x), \ldots) \in \mathbb{R}^k$ is uniquely defined.

Let $K_C = \{\lambda(x), x \in C, ||x|| = 1\} \subset \mathbb{R}^k$. This compact set is a subset of the set

$$\Delta_k^+ = \{y \in \mathbb{R}_+^k : y_1 \geq y_2 \geq \cdots \geq y_k \geq 0, \sum_{i=1}^{k} y_i = 1\}.$$

Besides, we have $\Delta_k^+ \subset \Delta_k$, where $\Delta_k = \{x \in \mathbb{R}_+^k \mid \sum_{i=1}^k x_i = 1\}$ is the $(k-1)$-dimensional probability simplex. We will also make an abuse of notation and also denote by K_C the subset of Δ_k that is obtained by symmetrizing K_C under permuting the coordinates.

For a positive real number $p > 0$, we recall that the *Rényi entropy of order p* of a probability vector $x \in \Delta_k$ to be

$$H^p(x) := \frac{1}{1-p} \log \sum_{i=1}^{k} x_i^p.$$

2010 *Mathematics Subject Classification.* 46L65 (46L37, 46L54, 46L87).

Key words and phrases. Free probability, Quantum Information Theory, Minimum Output Entropy additivity problem.

Since $\lim_{p\to 1} H^p(x)$ exists, we define the *Shannon entropy* of x to be this limit:

$$H(x) = H^1(x) = -\sum_{i=1}^{k} x_i \log x_i.$$

Note that the following are equivalent:

- C is entangled
- $(1, 0, \ldots 0)$ does not belong to K_C
- $\min_{x\in K_C} H^p(x) > 0$

1.2. **MOE and additivity.** One important motivation for studying entanglement comes from the Minimum Output Entropy problem. A *quantum channel* is by definition a linear completely positive trace preserving map $\Phi : \mathbb{M}_n(\mathbb{C}) \to \mathbb{M}_k(\mathbb{C})$. For a quantum channel $\Phi : \mathbb{M}_n(\mathbb{C}) \to \mathbb{M}_k(\mathbb{C})$, we define its *minimum output Rényi entropy (of order p)* by

$$H^p_{\min}(\Phi) := \min_{\substack{\rho\in\mathbb{M}_n(\mathbb{C}) \\ \rho\geq 0, trace\rho=1}} H^p(\Phi(\rho)).$$

where $H^p(\Phi(\rho)) := H^p(\text{eigenvalues}(\Phi(\rho))$.

The additivity problem -also known as *Minimum Output Entropy (MOE) additivity problem-* can be formulated as follows: for a given $p \geq 1$, do there exist two quantum channels Φ_1, Φ_2 such that

$$H^p_{\min}(\Phi_1 \otimes \Phi_2) < H^p_{\min}(\Phi_1) + H^p_{\min}(\Phi_2)?$$

The answer to this problem is affirmative: there exists such a pair of channels (Φ_1, Φ_2). It was proved by Hayden and Winter in the case $p > 1$, and by Hastings in the case $p = 1$ ([9, 11, 8]).

However there is no concrete counterexample so far: all available existence proofs rely on random techniques. Our aim is to explain the relation between this problem and Free Probability theory, and to show how results of Free Probability type in random matrix theory help to improve the bounds.

2. Random subspaces and free probability

2.1. **Random collection of eigenvalues.** Let k be an integer and $t \in (0, 1)$ be a real number. Let n be an integer less than kN. We assume that n is a function of N and that n, N vary and tend to infinity according to $n \sim tNk$.

Let V_N be a random subspace of dimension n of $\mathbb{C}^k \otimes \mathbb{C}^N$. In other words, V_N is a random element of the Grassman manifold of projections of rank n in $End(\mathbb{C}^{Nk})$, with respect to the invariant probability measure.

We are interested in the random set $K_{N,t,k} := \tilde{K}_{V_N}$ with the notations of the previous paragraph. Let us define the convex body $K_{t,k} \subset \mathbb{R}^k$ as follows:

$$K_{t,k} \subset \mathbb{R}^k := \{a \in \Delta_k, \forall b \in \Delta_k, \sum_{i=1}^{k} a_i b_i \leq ||pbp||_\infty\},$$

where p and b are seen as free selfadjoint elements of respective distribution $(1-t)\delta_0 + t\delta_1$ and $k^{-1}\sum \delta_{b_i}$ (see [14]). In [1], we proved

Theorem 2.1. *Almost surely, $dist(K_{N,t,k}, K_{t,k}) \to 0$, where dist is the Hausdorff distance between sets.*

2.2. **Random image, I.** For the needs of the sequel of the report, we will denote S_k as the collection of $k \times k$ self-adjoint trace 1 matrices. In Quantum Information theory, this is called the state space.

As in the previous subsection, k, t are fixed, and n, N go to infinity according to $n \sim tNk$, but this time, instead of choosing V_N at random, we choose a random isometry $W_N : \mathbb{C}^n \to \mathbb{C}^k \otimes \mathbb{C}^N$. For each N, the distribution of the law of the isometry follows the uniform probability distribution.

We consider the completely positive trace preserving (quantum channel) $\Phi_N : \mathbb{C}^n \to \mathbb{C}^k$ given by $\Phi_N(x) = (Tr_k \otimes id_N)W_N x W_N^*$.

Here we introduce the set $\tilde{K}_{t,k} \subset S_k$ of matrices A satisfying $Tr(Ax) \leq ||x||_{(t)}$ for any self-adjoint trace 1 matrix x. Following the lines of [1], we can prove

Theorem 2.2. *Almost surely, $dist(\Phi_N(S_N), \tilde{K}_{t,k}) \to 0$.*

Note that $\tilde{K}_{t,k}$ is the collection of selfadjoint matrices having eigenvalues in $K_{t,k}$.

2.3. **Random image, II.** Finally, we consider the setting where k is fixed and the map $\Phi_N : \mathbb{M}_N(\mathbb{C}) \to \mathbb{M}_k(\mathbb{C})$ is obtained as above, but where the random isometry $W_N : \mathbb{C}^n \to \mathbb{C}^k \otimes \mathbb{C}^N$ has the distribution of the block column matrix $k^{-1/2}(U_i)_{i=1}^k$, where the U_i are iid $N \times N$ Haar distributed random unitary matrices.

The probability model for the random quantum channel Φ_N of this section might look somewhat unnatural. However, this map is known in Quantum Information theory as the complementary of the map

$$\tilde{\Phi}_N(x) = k^{-1}(U_1 x U_1^* + \ldots + U_k x U_k^*),$$

and Φ_N and $\tilde{\Phi}_N$ share the same non-trivial eigenvalues when evaluated on rank one projector, therefore they have the same minimal output entropy. Actually, the map $\tilde{\Phi}_N$ is very close to the map that was originally constructed by Hastings in his first counterexample to the MOE additivity problem.

Next, we introduce the set K_k defined as being the subset of S_k given by matrices x such that $Tr(Ax) \leq ||pAp||$ for any $A \in S_k$, where $p = k^{-1}(u_i u_j^*)_{i,j=1}^k$, u_i are the generators of the reduced free group C^*-algebra $C^*_{red}(F_k)$ on k generators, and $||pxp||$ is understood as a norm on $\mathbb{M}_k(C^*_{red}(F_k))$. In [4], we prove

Theorem 2.3. *Almost surely, $dist(\Phi_N(S_N), K_k) \to 0$, where dist is the Hausdorff distance between sets.*

Note that here, unlike in the previous case, the image is not invariant under unitary conjugation by U_k. Remark also that in all cases considered in this section, the images are always convex sets. One can actually show that every point in the interior of the convex sets are almost surely in the image.

The main new technique to prove these results is an improvement on a famous result of [7], which we discuss in the next section.

3. Improvement on Haagerup and Thorbjornsen's results

We recall the following definitions from free probability theory.

(1) A *C^*-probability space* $(\mathcal{A}, .^*, \tau, \|\cdot\|)$ consists of a unital C^*-algebra $(\mathcal{A}, .^*, \|\cdot\|)$ endowed with a state τ, i.e. a linear map $\tau : \mathcal{A} \to \mathbb{C}$ satisfying $\tau[1_{\mathcal{A}}] = 1$ and $\tau[aa^*] \geq 0$ for all a in $\mathcal{A}$. In this paper, we always assume that τ is a trace, i.e. that it satisfies $\tau[ab] = \tau[ba]$ for every a, b in $\mathcal{A}$. A trace is said to be *faithful*

if $\tau[aa^*] > 0$ whenever $a \neq 0$. An element of $\mathcal{A}$ is called a (non commutative) random variable.

(2) Let $\mathcal{A}_1, \ldots, \mathcal{A}_k$ be $*$-subalgebras of $\mathcal{A}$ having the same unit as $\mathcal{A}$. They are said to be *free* if for all $a_i \in \mathcal{A}_{j_i}$ $(i = 1, \ldots, k,\ j_i \in \{1, \ldots, k\})$ such that $\tau[a_i] = 0$, one has

$$\tau[a_1 \cdots a_k] = 0$$

as soon as $j_1 \neq j_2$, $j_2 \neq j_3, \ldots, j_{k-1} \neq j_k$. Collections of random variables are said to be free if the unital subalgebras they generate are free.

(3) Let $\mathbf{a} = (a_1, \ldots, a_k)$ be a k-tuple of random variables. The *joint distribution* of the family $\mathbf{a}$ is the linear form $P \mapsto \tau\big[P(\mathbf{a}, \mathbf{a}^*)\big]$ on the set of polynomials in $2p$ non commutative indeterminates. By *convergence in distribution*, for a sequence of families of variables $(\mathbf{a}_N)_{N\geq 1} = (a_1^{(N)}, \ldots, a_p^{(N)})_{N\geq 1}$, we mean the pointwise convergence of the map

$$P \mapsto \tau\big[P(\mathbf{a}_N, \mathbf{a}_N^*)\big],$$

and by *strong convergence in distribution*, we mean convergence in distribution, and pointwise convergence of the map

$$P \mapsto \big\|P(\mathbf{a}_N, \mathbf{a}_N^*)\big\|.$$

(4) A non commutative random variable u is called a *Haar unitary* when it is unitary $(uu^* = u^*u = \mathbf{1})$ and for all n in $\mathbb{N}$, one has

$$\tau[u^n] = \begin{cases} 1 & \text{if } n = 0, \\ 0 & \text{otherwise.} \end{cases}$$

The following theorem was proved in [3], and improves on Haagerup-Thorbjornsen's result [7], that generalizes itself results of asymptotic freeness of [13]. It is the key ingredient to the proof of results in section 2.

Theorem 3.1. *For any integer $N \geq 1$, we consider*

- *a family $\mathbf{U}_N = (U_1^{(N)}, \ldots, U_p^{(N)})$ of $N \times N$ independent unitary Haar matrices,*
- *a family $\mathbf{Y}_N = (Y_1^{(N)}, \ldots, Y_q^{(N)})$ of $N \times N$ matrices, possibly random but independent of $\mathbf{U}_N$.*

In a C^*-probability space $(\mathcal{A}, .^*, \tau, \|\cdot\|)$ with faithful trace, we consider

- *a family $\mathbf{u} = (u_1, \ldots, u_p)$ of free Haar unitaries,*
- *a family $\mathbf{y} = (y_1, \ldots, y_q)$ of non commutative random variables, free from $\mathbf{u}$.*

Then, if $\mathbf{y}$ is the strong limit in distribution of $\mathbf{Y}_N$, we have that $(\mathbf{u}, \mathbf{y})$ is the strong limit in distribution of $(\mathbf{U}_N, \mathbf{Y}_N)$.

A partial version of this result had been conjectured by Pisier and Haagerup almost ten years ago. As a corollary we have:

Corollary 3.1. *Let Q_n be a random projection of rank n in $\mathbb{M}_{Nk}$ and let A be the diagonal matrix $diag(a_1, \ldots, a_k) \otimes I_N$. Then the operator norm of Q_nAQ_n converges almost surely to $\phi((a_i), t)$ as $N \to \infty$.*

This corollary was initially obtained in [1] and it was sufficient for the purposes of models of subsections 2.1 and 2.2, but it follows from the more general Theorem 3.1

The idea to use results of almost sure convergence in operator norm of random matrices for the MOE additivity problem first appeared in [6], where the non-additivity of the MOE is reproved and extended in the case $p > 1$.

4. Violation of additivity

It follows from the above theorems that the minimum output entropy is a quantity that converges almost surely. More precisely,

Theorem 4.1. *For any of the three models considered above, $H^p_{\min}(\Phi_n)$ towards the minimum of H^p on the limiting set $K_{t,k}$ (resp. $\tilde{K}_{t,k}, K_k$).*

It is of natural interest to study the convex ball $K_{t,k}$ and in particular the minimum of Rényi functions on it. Based on extensive numerical simulation, we conjecture:

Conjecture 4.1. *For any $k \geq 183$ there is a violation of the MOE additivity. The violation happens almost surely with the Bell state iff $k \geq 183$, and this violation can be made as close as possible to* $\log 2$.

5. Additional remarks

The techniques presented in this note have actually many other applications to the theory of operator algebras and quantum information theory. For example, it gives a systematic way of producing k-positive maps, it allows to understand the image of an arbitrary family of orthogonal pure states under Φ_n and therefore to show that the Holevo capacity also converges almost surely, and it allows to understand the behaviour of random unitary channel. All these further applications are the object of work in preparation.

References

[1] Belinschi, S., Collins, B. and Nechita, I. , *Laws of large numbers for eigenvectors and eigenvalues associated to random subspaces in a tensor product* math/arXiv:1008.3099 - to appear in Inventiones Mathematicae.

[2] Collins, B., *Product of random projections, Jacobi ensembles and universality problems arising from free probability* Probab. Theory Related Fields, 133(3):315–344, 2005.

[3] Collins, B., Male, C. *The strong asymptotic freeness of Haar and deterministic matrices* math/arXiv:1105.4345

[4] Collins, B., Fukuda, M., Nechita, I. *Towards a state minimizing the output entropy of a tensor product of random quantum channels* arXiv:1111.6269 - to appear in Journal of Mathematical Physics

[5] Collins, B. and Nechita, I., *Random quantum channels I: Graphical calculus and the Bell state phenomenon.* Comm. Math. Phys. 297 (2010), no. 2, 345-370.

[6] Collins, B. and Nechita, I., *Random quantum channels II: Entanglement of random subspaces, Rényi entropy estimates and additivity problems* Advances in Mathematics 226, 11811201 (2011)

[7] Haagerup, U. and Thorbjørnsen, S., *A new application of random matrices:* $\mathrm{Ext}(C^*_{\mathrm{red}}(F_2))$ *is not a group.* Ann. of Math. (2) 162 (2005), no. 2, 711–775.

[8] Hastings, M.B., *A Counterexample to Additivity of Minimum Output Entropy* arXiv/0809.3972v3, Nature Physics 5, 255 (2009)

[9] Hayden, P., *The maximal p-norm multiplicativity conjecture is false* arXiv/0707.3291v1

[10] Hayden, P., Leung, D. and Winter A., *Aspects of generic entanglement* Comm. Math. Phys. 265 (2006), 95–117.

[11] Hayden, P. and Winter A., *Counterexamples to the maximal p-norm multiplicativity conjecture for all $p > 1$.* Comm. Math. Phys. 284 (2008), no. 1, 263–280.

[12] Ledoux, M., *Differential operators and spectral distributions of invariant ensembles from the classical orthogonal polynomials part I: the continuous case.* Elect. Journal in Probability 9, 177–208 (2004)

[13] Voiculescu, D.V., *A strengthened asymptotic freeness result for ran- dom matrices with applications to free entropy* Internat. Math. Res. Notices, (1):41-63, 1998.

[14] Voiculescu, D.V., Dykema. K.J. and Nica, A., *Free random variables*, AMS (1992).

B.C.: RIMS, KYOTO UNIVERSITY, AND DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OTTAWA, 585 KING EDWARD, OTTAWA, ON K1N 6N5, CANADA AND CNRS, FRANCE
E-mail address: bcollins@uottawa.ca